UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

Wireless Local Area Network Security Protocols: Compliance with the IEEE 802.11i Standard

CAPSTONE REPORT

Robert Reilly
Manager of Network Technology
Federated Systems Group

University of Oregon
Applied Information Management
Program

June 2005

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger

Academic Director, AIM Program

Abstract for:

Wireless Local Area Network Security Protocols:

Compliance with the IEEE 802.11i Standard

As Government regulations become more stringent, corporate responsibility to ensure data privacy increases. This study analyzes selected literature published between 1997 and 2005 to provide an analysis of wireless local area network security protocols based on compliance with criteria in the IEEE 802.lli standard. Capabilities, vulnerabilities and components are compared, to help IT executives form corporate security policy. Three protocols examined are Wired Equivalent Privacy, Wi-Fi Protected Access and Extensible Authentication Protocol-Transport Layer Security.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I – PURPOSE OF STUDY

Brief Purpose

The purpose of this study is to provide an analysis of wireless local area network security protocols (Arbaugh & Edney, 2004, p. 17) based upon their compliance to the criteria specified in the IEEE 802.11i standard (Halasz, 2004; Funk, 2005; Javvin, n.d). Specifically, this study compares the three wireless local area network security protocols defined in the IEEE 802.11 (Andress, 2002; Chandra, 2002), IEEE 802.1x (Snyder, 2002; searchMobileComputing.com 2003) and WiFi Institute (Cheung, 2004; Omatseye, 2003; Wildstrom, 2002) standards in term of their capabilities in the areas of authentication, encryption and key management as defined in the IEEE 802.11i standard (Halasz, 2004; Funk, 2005; Javvin, n.d).

While the content presented in this study may be of use to a broader audience, it is specifically focused on information technology managers who hold responsibility for developing security policy for corporate wireless local area networks. As the number of wireless local area networks deployed by corporations has grown (Hollis, 2004; Nair, 2003; Jason 2003) information technology managers now cite security as their primary concern when considering the deployment of wireless local area networks in their organizations (Disabato, 2003; Greene, 2003; Nair, 2003; Molta, 2002). Driven by legal and regulatory responsibilities, it is critical for corporations to maintain data integrity and ensure personal privacy (Parenty, 2003; Dix, 2004; Johnson, 2004; Garretson, 2003).

The larger method of study is literature review (Leedy and Ormod, 2001). Literature review is chosen as an appropriate method for this study because the majority of data that exists for these technical disciplines exist in written form published in technical journals, trade publications, academic research and as a result of studies performed by professional societies. Literature was collected from materials published between January 1997 and April 2005 pertaining to the following bodies of knowledge:

- Wireless Local Area Network security protocols (Chandra, 2002; Omatseye, 2003)
- Wireless Local Area Network standards (Funk, 2005; Andress, 2002)
- Wireless Local Area Network security risks (Arbaugh, & Edney, 2004; Parenty, 2003)
- Wireless Local Area Network market information (Hollis, 2004; Nair, 2003)
- Corporate data privacy regulations and responsibilities (Dix, 2004; Johnson, 2004)

Once obtained, specific resources are subjected to content analysis (Krippendorff, 2004) as a qualitative framework for building a base of knowledge on the definitions, specifications, characteristics, capabilities, vulnerabilities and operability of the bodies of knowledge outlined above. Results of the content analysis are categorized into topic groupings and examined to discover trends evidenced within the specific data, uncover inconsistencies and ultimately define a common structure for each of the topics areas of focus based upon the sources listed in the bibliography.

The results of the content analysis are framed into two primary outcomes: (1) an annotated bibliography of published sources relating to the purpose of the study and (2) a table showing the capabilities of the protocols studied with respect to the criteria defined in the 802.11i standard. These two outcomes serve as a structured and clearly cited resource for IT executives with responsibility for defining corporate data security to understand the governing standards for the wireless local area networks and the security protocols defined in these standards. The intent is that these IT executives will be able to use these outcomes as decision making tools when designing corporate wireless local area network security policy.

Full Purpose

Significance

As the wireless local area network market has grown (Kim, & Porter, & Kittipom, 2005; Hollis, 2004) industry concerns about the security of wireless local area network technology have also increased (Le Thomas, 2004; Snyder, & Thayer, 2004). In fact, already several years ago a study conducted by the Gartner Group in 2002 stated, "by the end of 2002, 30 percent of all enterprises will risk security breaches because they've deployed 802.11b wireless local area networks (WLANs) without proper security." (Chandra, 2002; http://www.wirelessdevnet.com/articles/80211security/**).** This risk, coupled with several high profile breaches of data security and privacy on corporate networks (Garretson, 2003; Albright, 2003**)** has resulted in new legislation regulating the way corporations must guard privacy and insure data security in their organizations (Dix, 2004; Ferguson, 2005). These regulations range from industry-specific legislation such as

the Health Information Portability and Accountability Act (HIPPA) and Gramm-Leach-Bliley (GLBA) Act to corporate-wide legislation including Sarbanes-Oxley and California SB1386 (Garretson, 2003). (For the purpose of this study, privacy is defined as freedom from unauthorized intrusion (http://www.m-w.com/cgi bin/dictionary?book=Dictionary&va=privacy).)

For the companies that are regulated by this legislation, the consequences for not having a plan for protecting data are serious and include:

- Legal action (Reed, 2004; Davies, 2003)
- Fines from regulatory non-compliance (Vijayan, 2003; Davies, 2003)
- Loss of customer and industry confidence (Vijayan, 2003; Mastroberte, 2003)
- An inability to do business in certain parts of the world (Vijayan, 2003)

Nobody understands this risk more acutely than the IT executives who hold responsibility for ensuring privacy and protecting corporate data (Brewin, 2003; Greene, 2003; Snyder & Thayer (2004, October 4)). In fact, in a 2005 poll, Network Computing Magazine subscribers rated security concerns and uncertainly over standards as the two most significant obstacles to the deployment of wireless local area networks (Molta, 2005). This level of concern over wireless local area network security (Molta, 2002; Le Thomas, 2004; Snyder & Thayer, 2004), coupled with the consequences IT executives face when corporate networks are breached (Ferguson, 2005; Goodwin, 2004), make these individuals the target audience for this study and those who will most benefit from its content. In addition, this study may also benefit corporate executives from outside the

IT department who, as a result of the legislation discussed above, are now legally accountable for their organizations' adherence and ultimately culpable for any breaches that occur (Dodds, & Hague, 2004; Davies, 2003; Barrett 2000).

The purpose of this study is to analyze the wireless local area network security protocols (Arbaugh & Edney, 2004, p. 17) defined in the Institute of Electrical and Electronics Engineers standards (IEEE) 802.11(Andress, 2002; Chandra, 2002), IEEE 802.1x (Snyder, 2002; searchMobileComputing.com 2003) and Wi-Fi Alliance (Cheung, 2004; Omatseye, 2003; Wildstrom, 2002) using as criteria the authentication, encryption and key management security models defined in the IEEE 802.11i standard (Halasz, 2004; Funk, 2005; Javvin, n.d). Specifically, three protocols are analyzed; Wired Equivalent Privacy, Wi-Fi Protected Access and Extensible Authentication Protocol-Transport Layer Security.

In order to better understand the scope and purpose of this study a deeper understanding of the standards and protocols referred to above is necessary. In this study a standard is defined as "something established by authority, custom, or general consent as a model or example" (http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=standard). The protocols and standards analyzed in this study have been chosen because of their connection with the IEEE, IETF and Wi-Fi Alliance, the organizations responsible for developing the standards that define the wireless network industry (A brief history of Wi-Fi, 2004; http://www.hifn.com/support/Glossary_I.html). The IEEE is a professional organization

made up of engineers and scientists from industry and academia for the express purpose of developing, publishing and maintaining technical standards (http://encyclopedia.laborlawtalk.com/IEEE; http://whatis.techtarget.com/definition/0,,sid9_gci214016,00.html). The Wi-Fi Alliance is a global cooperative of wireless manufacturers created for the purpose of promoting the growth of wireless local area networks (Snyder, & Thayer, 2004, October 4). The IETF, an acronym for the Internet Engineering Task Force, is the professional organization responsible for the development and publishing of standards related to Internet technology (http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftglossary.htm). The selection of these standards also ensures that no proprietary protocols are included which might undermine the credibility of the study.

Wireless Network Standards

The IEEE 802.11 standard, published in 1997 (Gast, 2002), was the first wireless local area networks standard created (Champness, 1998). Initially envisioned for wireless networks of limited size, the original standard restricted communication to the one and two Megabits per second frequency bands (Riezenman, 2002). However, in order to keep pace with technical and business changes in the WLAN industry since 1997, the standard has been enhanced several times (Riezenman, 2002). Recognized as the most significant event in the history of wireless local area networking, the 802.11 standard has provided the foundation for all the WLAN technologies that have followed (A brief history of Wi-Fi, 2004).

The Wi-Fi Alliance standard, released in 2003, was created for the express purpose of providing an interim solution for wireless local area network security between the publishing of the 802.11 and 802.11i standards (Pabrai & Uday, 2004; Wildstrom, 2002). The purpose for the creation of this standard was industry concern over the security and reliability of the WEP protocol defined in the IEE 802.11 standard (Roberts, 2003).

The 802.1x standard, published in 2001, was developed by the IEEE to provide enhanced security for 802.11 networks (Snyder, 2002) by defining a new framework for centralized user authentication and key management (Geier, 2003; searchMobileComputing.com Definitions, 2003). Originally planned as an authentication standard for wired local area networks only, 802.1x was revised prior to its release to include authentication for wireless local area networks as well (Arbaugh & Edney, 2004. pg 122-124, 127-129). This decision was made by the IEEE in response to problems uncovered in the security methodology for the IEEE 802.11 standard (Geier, 2003; Huckaby, 2001). Compared to the other standards defined in this study 802.1x is unique in the way in which it incorporates existing standards into its methodology to provide a more robust security model (Snyder & Thayer, 2004; Geier, 2003; Huckaby, 2001).

The standard that provides the criteria for this study is IEEE 802.11i. Published in 2004, 802.11i represents the latest addendum to the original 802.11 standard focusing solely on the security of wireless local areas networks (Bauer, 2005; Arbaugh & Edney, 2004). Referred to as the Robust Security Model, 802.11i standard was expressly created

to define a comprehensive method for securing WLAN's based upon authentication, encryption and key management (Arbaugh & Edney, 2004; Cohen & O'Hara, 2003).

Wireless Network Protocols

The three security protocols selected for analysis in this paper are Wired Equivalent Privacy, Wi-Fi Protected Access and Extensible Authentication Protocol-Transport Layer Security. In the context of this study a protocol is defined as "A formal description of message formats and rules that two or more computers must follow in order to communicate across a network." (http://archive.ncsa.uiuc.edu/Cyberia/MetaComp/MetaGlossary.html). The earliest of the WLAN security protocols is Wired Equivalent Privacy, commonly referred to by the acronym WEP (Arbaugh & Edney, 2004. pg 67). WEP was developed in 1997 as part of the IEEE 802.11 standard for wireless local areas network technology (Riezenman, 2002). The initial goal of the IEEE in creating WEP was to provide a method for securing wireless local areas networks equal to those that existed for wired local area networks (http://www.netstumbler.com/faqs/dictionary/wep/). Specifically, WEP defines a method for providing authentication, encryption and key management on wireless local area networks (Arbaugh & Edney, 2004. pg 69).

The next phase of wireless local area network security occurred in 2003 with the creation of the Wi-Fi Protected Access, or WPA, protocol by the Wi-Fi Alliance (Omatseye, 2003; Snyder & Thayer, 2004). In order to address perceived vulnerabilities of WEP, and in reaction to the release of the IEEE 802.11i draft standard (Cheung, 2004**;**

Roberts, 2003; Snyder & Thayer, 2004, October 4), the Wi-Fi Alliance designed WPA as an more robust security solution for wireless local area network security which would replace WEP (http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf; Passmore, 2004; Roberts, 2003) and be forward compatible with the 802.11i standard (http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf; Omatseye, 2003). Functionally, the WPA protocol defines a method for securing wireless local area networks by providing standards for authentication and encryption (Wildstrom, 2002; Wi-Fi Protected Access, 2005).

The final protocol analyzed is Extensible Authentication Protocol-Transport Layer Security, also referred to as EAP-TLS. Unlike WEP and WPA, Extensible Authentication Protocol-Transport Layer Security is a hybrid protocol coupling two distinct security standards, EAP for authentication and TLS for encryption, into a single security solution (Balinsky, & Miller, & Sankar, & Sundaralingam, 2005; Dornan, 2004). Another unique quality of EAP-TLS is that although EAP-TLS as a protocol was first defined as a result of the publication of the 802.1x standard the individual protocols of EAP and TLS were defined by a standards society other that the IEEE and predate 802.1x by several years (http://www.faqs.org/rfcs/rfc2246.html; http://www.faqs.org/rfcs/rfc2716.html). Although over 20 extensions to the EAP standard exist (Dornan, 2004) only EAP-TLS was chosen for this study. The reason for this decision is that EAP-TLS is the only EAP extension that has been accepted as a standard by the Internet Engineering Task Force (IETF) (Dornan, 2004; http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/draft/draftglossary.htm).

Functionally, EAP-TLS defines a method for securing wireless local area networks by providing standards for authentication, encryption and key management (Dornan, 2004; Geier, 2003; IETF, 1999).

Using literature review (Leedy and Ormod, 2001) as the overarching research methodology, resources are collected from the following bodies of knowledge:

- Wireless Local Area Network security standards. This area includes data on the specifications, history and functionality of WLAN standards as well as background information of the organizations that developed these standards.
- Wireless Local Area Network security protocols. Data in this area focus on the security protocols defined as part of the WLAN standards. Specific areas of focus will be functionality, vulnerabilities and risk.
- Wireless Local Area Network security risks. This data focuses on sources related to the risks associated with the deployment and operation of wireless local area networks. These risks include breach of privacy, data integrity, regulatory responsibilities and malicious attacks.
- Wireless Local Area Network market information. This data provides context for the size and importance of the WLAN market in the corporate environment. Data on factors including market growth, deployed base, market projections and scope of implementation are gathered.
- Corporate data privacy regulations and responsibilities. These data examine the regulations and legislation that exist to ensure corporations ensure data privacy.

Additional areas of focus are management responsibility, corporate security policy development and the consequences for non-compliance.

Once collected, the data gathered are organized and analyzed using content analysis. As defined by Krippendorff, content analysis "is a research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use" (Krippendorff, 2004, pg. 18). Using problem-driven content analysis, defined by Krippendorff as "epistemic questions about currently inaccessible phenomena, events, or processes, that the analysts believe texts are able to answer" (Krippendorff, 2004, pg. 342-343), the research process was divided into five stages:

- Research Question Formulation. This stage of the research process defines the over arching research questions that proved the foundation for the research process (Krippendorff, 2004, pg. 343).
- Research Criteria. This stage of the process builds on the research questions defined in stage one by defining the precise criteria to be researched (Leedy & Ormrod, 2001, pg. 156). Criteria take the form of a set of key words and phrases that represent all pertinent characteristics of the bodies of knowledge.
- Data Collection. This stage of the research process uses the list of key words and phrases developed in stage three to build queries to search for data (Krippendorff, 2004, pg. 347-349). The result of this stage is the building of the resource list that provides the information base for the study and the organization of these resources based upon their relationship to the categories of security, protocols, market, privacy and standards.

- Data Analysis. This stage uses a qualitative analysis of the sources gathered in the data collection stage to review the material in each of the categories defined in the data collection stage. The goal of this stage is to use criteria including frequency of occurrence, consistency of information and strength of the source to create a build a base of knowledge on the definitions, specifications, characteristics, capabilities, vulnerabilities and operability of the standards and protocols that represent the focus of the study (Krippendorff, 2004, pg. 349-353; Leedy & Ormrod, 2001, pg. 156-157).
- Outcomes. Two outcomes are planned from the completion of this process. The first is the creation of an annotated bibliography, organized by their relevance to the categories of security, protocols, market, privacy and standards. The second outcome is the creation of a table representing the definitions, specifications, characteristics, capabilities, vulnerabilities and operability of the three security protocols analyzed based upon the three criteria defined in the IEEE 802.11i standard. It is the intention of the researcher that these two outcomes will be used by IT executives responsible for developing corporate security policy as a reference when developing corporate security policy.

Limitations

The literature used for this study is limited to sources published between January 1997 and April 2005. This earlier date is selected because it coincides with the development date of the earliest of the standards and protocols. The later date is selected in order to ensure the most current information was being referenced and well as allowing

for the broadest possible time frame. This broader time frame allows the researcher to gather sources relevant to the time of their development as well as obtaining a historical perspective of the topics over time.

To further ensure the quality and credibility of the references only published literature from the following sources is used:

- Technical journals
- Industry papers
- Professional Society Proceedings
- Conference Notes
- Academic Papers
- Books

These references are selected because of their significance to the focus areas of the study and because they contained the proper degree of technical and business information relative to standards, protocols, privacy, security and regulations.

With the same goal of ensuring the strength and credibility of the literature the following sources are not considered. Specifically, these sources are excluded because their reliability and lack of bias cannot be verified. In addition, these sources lack the requisite level of references or independent focus necessary to render their information credible and factual.

- Opinion/Editorial pieces
- Corporate Marketing Material

- Unpublished books, articles or white papers
- BLOG's.

Regarding purpose and focus, this study is designed to:

- Focus on standards defined by the IEEE, IETF and Wi-Fi Alliance
- Include only protocols adhering to an 802.11 standard
- Appeal to a general corporate/industry base
- Use only those criteria specified in the 802.11x standard
- Present an analysis of the WEP, WPA and EAP-TLS protocols based upon their capabilities in the areas of authentication, encryption and key management
- Provide IT executives responsible for the development of security policy with a framework for understanding the functionality of the WEP. WPA and EAP-TLS protocols for application on their specific environments
- Focus on the key areas of WLAN standards, WLAN security protocols, the WLAN market and corporate privacy

It is important to note that this study is not designed to:

- Address a specific industry or customer base. This limitation ensures the data contained in the study appeals to the broadest possible corporate base making its data more accessible and applicable.
- Address specific applications or implementations of the technologies. Specific applications of the protocols analyzed in the study will be left to the IT executives

who make up its audience. Any attempt by the researcher to frame this paper to a specific implementation would be counter to the purpose.

- Cover the technical details of algorithms. This limitation ensures the data is presented at the proper level of detail for the IT executives that make up its audience. Including technical specifications for the individual algorithms are out of the scope and technical acumen of these IT executives.
- Discuss proprietary standards or protocols. This strengthens the overall credibility of the study by ensuring a strict adherence to industry standards.
- Discuss vendor specific products or services. As the protocols analyzed in the study are defined and regulated by industry standards that are non-proprietary the inclusion of vendor specific products is unnecessary.
- Provide a ranking or rating system for the protocols. As no specific statistic or methods exist for developing a rating or rankling systems any attempt to do so would not be rooted in standards or mathematical certainty.
- Provide a recommendation on which protocol to use. As no statistical method exists for developing accurate, reliable rankings any recommendations would be speculative and opinion based undermining the credibility of the study.

Problem Area

High profile security breaches at Best Buy, Lowe's Bank of America Corp., ChoicePoint Inc. and LexisNexis Group have highlighted the exposures that exist in corporate data security (Kumar 2005; Tolly 2005). These breaches impact consumer confidence and prompt State and Federal governments to enact new legislation regulating

corporate responsibilities for ensuring privacy and maintaining data security (Garretson, 2003). In fact, The National Strategy to Secure Cyberspace released by The White House in 2002, and revised in 2003, (http://www.whitehouse.gov/pcipb/) stressed the need for the creation of "common criteria" for defending governmental, corporate and private IT resources as a national security imperative (Messmer, 2003).

These new regulatory burdens regarding privacy have also created a heightened awareness for IT executives and corporate officers with regard to the security of networks in general and wireless local area networks in particular (Brewin 2003; Parenty 2003; Nair, 2003). Recent studies conducted by the Gartner Group show IT executives rate security concerns as the largest inhibitor to the deployment of wireless local area networks in their organizations (Vijayan 2004; Snyder & Thayer 2004; Disabato, 2003). Perhaps of greatest concern for these executives are the professional and personal consequences of regulatory non-compliance (Davies 2003). Legislation like (1) Sarbanes-Oxley, (2) The Health Information Portability and Accountability Act (HIPPA), (3) The Gramm-Leach-Bliley (GLBA) Act and (4) and California SB1386 now place personal responsibility for ensuring corporate data privacy on specific individuals (Kumar, 2005; Ferguson 2005) making the cost of non-compliance considerable including potential legal action, fines and in some cases incarceration (Cheek 2005; Davies 2003).

The development of a comprehensive corporate IT security policy is among the most critical tasks organizations face today (Kumar, 2005; CIO Insight, 2004; Vijayan 2003). Among the most critical areas for IT executive who hold responsibility for

ensuring corporate data security to address is the organizations wireless local area networks (Rist 2005; Goodwin, 2004). Unlike most other corporate assets that can be protected by limiting access via secure enclosures or physical limitation to the resource, wireless local area networks have no physical resources to restrict intrusive access to (Steinke 2002; Marek, 2001). The transmission medium (http://www.atis.org/tg2k/_transmission_medium.html) for 802.11 wireless networks is open radio frequencies, openly accessible to any device with hardware compatible with the 802.11 standard (Albright 2003; Arbaugh & Edney, 2004). This method of transmission, coupled with the rapid growth of the technology (Kim, & Porter, & Kittipom, 2005; Hollis, 2004), makes the security of wireless local area networks a unique challenge when developing IT security policy (Case, 2004; Economist, 2002). The ubiquitous nature of wireless local area network technology, particularly in the consumer market, (Webb, 2003; Brewin, 2002) heightens this risk by building a base of potential hackers outfitted with the tools and knowledge (Air Defense, 2005; Economist, 2002) for executing malicious attacks on corporate WLAN's from outside of the organizations' physical facilities (Arbaugh & Edney, 2004; Albright, 2003). Additionally, as the deployment of wireless local area networks has grown in corporations (Motsay, 2004; RCR Wireless News, 2004; Garcia, 2003) so too has the sensitivity of data these networks carry (Kumar, 2005; Albright, 2003).

Understanding the risks that exist to the corporate wireless local area network is a first step that IT executives face when determining corporate security policy (Goodwin, 2004; Albright, 2003). Once these executives understand the risks that exist in their

organizations, the next challenge is to understand the standards that exist relating to wireless local area network security (Balinsky & Miller & Sankar & Sundaralingam, 2005; Arbaugh & Edney, 2004). While a wealth of information exists for each of these standards, there remains a lack of understanding by IT executives on the characteristics of these standards (Molta, 2005; Snyder, & Thayer, 2004; Greene, 2003). This need is most pronounced when discussing the capabilities of the security protocols defined in these standards (Pabrai & Uday, 2004; Davies, 2003) as it is these protocols that provide the foundation for ensuring security and privacy on a wireless local area network (Arbaugh & Edney, 2004; Vijayan, 2004).

CHAPTER II – REVIEW OF REFERENCES

This section provides a review of the key references used to define the framing, purpose, problem area and research method of the study. In order to present these references in a manner that is clear, concise and easily referenced, the sources are categorized based upon their pertinence to the central topics of the study:

- WLAN standards and security protocols
- WLAN market
- Corporate privacy regulations, risks and responsibilities

In addition, a fourth section is included for sources related to the definition of the research methodology for the study.

Within these categories, each reference is annotated according to three points:

1. The specific content used in this study;
2. How this content is used as support within the following parts of the study:
    - The purpose of the study including the study's significance, scope and limitations
    - The problem area of the study
    - The method of the study
3. The criteria used for selection, including validity, pertinence and reliability.

As these references represent only a small percentage of available sources, careful consideration is given to their selection. The references included in this section are chosen based upon the following criteria:

- Amount of data contained in the reference. Sources were chosen based upon the amount of data, and level of detail contained in the reference.
- Completeness of the content. This criterion specifies the level of completeness of the data covered. Those sources containing only general overviews were excluded.
- Pertinence to the purpose of the study. This criterion looks at the sources pertinence to the central topics of the study's purpose, specifically standards, protocols, risks and method.

References Related to WLAN Standards and Security Protocols

Arbaugh, W. A., & Edney, J. (2004). *Real 802.11 Security.* Boston: Pearson Education Inc.

This text provides the foundation for research used in this study pertaining to wireless local area network standards and protocols. Arbaugh and Edney present detailed information on WLAN standards, WLAN security protocols and security policy development. The material presented in the book also facilitates the process of defining the boundaries of the study, as well as setting the boundaries of what would be examined. This source is selected based upon reviews the text received from the IETF, IEEE and Wi-Fi Alliance. The text's two authors are both accomplished members of the wireless community. Dr. William Arbaugh is Assistant Professor of Computer Science at the

University of Maryland and Jon Edney is a member of the IEEE 802.11 TGi security group.

Material from this source is used in the purpose section to define the characteristics of WLAN standards and protocols, specifically those that make up the focus of the study. This source is also used to define the limitations of the study by helping the researcher determine the correct standards to include.

Balinsky, A., & Miller, D., & Sankar, K., & Sundaralingam, S, (2005). Cisco Wireless LAN Security. Indianapolis: Cisco Press

This text provides an overview of the steps for developing a wireless local area network security model. Balinsky et al. present a comprehensive overview of the 802.11, 802.11i, and 802.1X wireless local area network standards, as well as information on the WEP and EAP security protocols. Additional information includes wireless network deployment, security configuration, risks and vulnerabilities. This reference was selected because of its content in the areas of WLAN protocols and standards, specifically the way these protocols and standards are important to the development of corporate security policy. The text is published by Cisco Press, a division of Cisco Systems, and written by four senior Cisco Systems engineers, each with greater than 15 years' experience with wireless network technology and security. The authors were assisted by four technical reviewers, including a senior security architect for Cisco and Dr. Peter Welcher who holds a Ph.D. in mathematics for MIT and is a former professor at the U.S Naval Academy.

Material from this source is used in the purpose section to help the researcher understand the WLAN standards and protocols. It is useful in the way it presents a comparison of the different standards based upon their encryption, authentication and key management capabilities. This resource is also used in the problem area to define the importance of wireless networks in the formulation of a corporate security policy.

Dornan, A. (2004, January). EAP: Extending Authentication to the Wireless LAN. Network Magazine, Vol. 19 Issue 1, p38

This article provides information on the EAP protocol and its derivatives. The author begins by outlining the different IEEE WLAN standards, focusing primarily on the IEEE 802.1X standard and EAP protocol. The primary data in the article centers on the five major EAP variants, including the one researched in this study, EAP-TLS. The resource defines the characteristics of EAP-TLS in relation to encryption and authentication. This article was published in Network Magazine, a leading industry magazine providing information on network technology and the networking market for IT management. The author of the article, Andy Dornan, is the chief technology editor at Network Magazine and the author of several books on wireless communication.

This article is used in the purpose section to define the characteristics of the EAP-TLS protocol as well as providing the justification of its inclusion in the study over the other EAP variants.

Geier, J. (2003, May 7). 802.1X Offers Authentication and Key Management. Retrieved on March 23, 2005 from http://www.wifiplanet.com/tutorials/article.php/1041171

In this article Geier presents an overview of the functionality and operability of the EAP protocol and 802.1X security standard in terms of there ability to provide secure data encryption. The article also points out the need to couple EAP with an authentication protocol such as TLS in order to provide a comprehensive security method. To underscore the strengths of the 802.1X standard, Geier contrasts it with its predecessor, WEP, defining the functionality of EAP in terms of authentication, encryption and key management. The article was selected based upon the strength and reputation of its author, Jim Geier. Geier is a voting member of the Wi-Fi Alliance, a past Chairman of the IEEE Computer Society and Chairman of the IEEE International Conference on Wireless LAN Implementation. Mr. Geier is also a member of the IEEE 802.11 working group responsible for developing wireless local area network standards.

This article is used in the purpose section to define to functionality of the EAP protocols and aided the researcher in selecting EAP-TLS as the EAP variant to be included in the study.

Halasz, D. (2004, August 25). IEEE 802.11i and wireless security. Retrieved on March 23 from http://www.embedded.com//showArticle.jhtml?articleID=34400002

In this article Halasz begins by providing an overview of the IEEE 802.11i WLAN security standard, contrasting it to the protocols that preceded it and providing a

justification for its development. Halasz then walks the reader through the standards for encryption, authentication and key management methods, finishing with a detailed description of the communication flow between the host and authentication device. The article was obtained from the embedded.com web site, the electronic version of Embedded Systems Programming magazine. The author, David Halasz "served as the chair of the IEEE 802.11i Task Group from its inception through the amendment's ratification in June of 2004".

This resource is used in the purpose sections to define the functionality of 802.11i and for the selection of this standard as the foundation for the study. The data helped the researcher to frame the study and serves as the common comparison for each of the security protocols studied.

Cheung, D. (2004, June). WLAN Security & Wi-Fi Protected Access. Dr. Dobb's Journal: Software Tools for the Professional Programmer, Vol. 29 Issue 6

In this article Cheung provides a detailed analysis of the functionality of the Wi-Fi Protected Access (WPA) WLAN security protocol as it relates to authentication and encryption comparing and contrasting these functions with those offered by the WEP. The author also looks at the justification behind the protocols development and the influence of the Wi-Fi Alliance in its development. Finally, Cheung walks through WPA's compatibility with emerging standards and protocols such as IEEE 802.1X and EAP. This article was obtained from Dr. Dobbs Journal; a technical magazine focused on the application developers and IT executives with the largest publication of any developer magazine. Cheung is a regular contributor to the magazine and an IT consultant.

Information from this resource is used in the purpose section to define the functionality of the WPA protocol in the areas of encryption and authentication. The researcher also used this article to justify the inclusion of WPA and the Wi-Fi Alliance standard, in the study.

References Related to the WLAN Market

Molta, D. (2005, February 17). WLANs Bust Out. Network Computing, Vol. 16 Issue 3, p37-42

This magazine article contains information on the size, current growth rate and future growth projections for the wireless local area network market in both the corporate and private sectors. The article also contains information on market direction, areas of opportunity and market players. Finally, the article briefly presents management concerns regarding WLAN technology. This article was published in Network Computing, a widely published and respected magazine that focused on network technology and the networking market. The author of the article, Dave Molta, is Assistant Dean of Technology Integration, Director of the Center for Emerging Network Technology and an Assistant Professor at Syracuse University in New York.

Information from this article is used in the purpose section to (1) define the size and direction of the WLAN market, (2) discuss the challenge to IT managers in reference to WLAN technology and (3) outline the concerns of IT managers in reference to WLAN deployment.

RCR Wireless News (2004, February 2). WLAN growth expected to continue through 2006. Vol. 23 Issue 5, p21, 1/9p

This article from the RCR Wireless News reports on a February 2004 study by the Dell'Oro Group on the growth of wireless local areas network market from 2004 through 2006. The study describes the projected increase in the enterprise WLAN market as a result of the adoption of the technology by corporations. The article was chosen based upon the reputation of the Dell'Oro Group, a market research company for the telecommunications industry, and their position in the industry.

Data from this resource is used in the purpose and problem sections to define the growth of the WLAN market and its penetration into the corporate environment.

References Related to Corporate Privacy Regulations, Risks and Responsibilities

Albright, B. (2003, March). Wireless insecurity. Frontline Solutions, Vol. 4 Issue 3, p16-19

This article provides an overview of WLAN standards, protocols, security policy and vulnerabilities from a business and management perspective. The article is structured and written in non-technical terms, in order to communicate to IT managers. It provides examples of existing standards and protocols that exist, the differences between wired and wireless local area networks, the challenges to securing wireless local area networks and the risks and consequences of breaches to these networks. The article is printed in Frontline Solutions magazine, a leading trade magazine for the supply chain management

industry. The author is an Associate Editor for Frontline Magazine specializing in wireless local area networks and mobile computing.

This article is used in the purpose section to outline the risks posed by wireless local area networks. The article is also used in the Problem Area to state the challenges, and importance, of securing wireless local area networks as well as to show the high profile breaches to WLAN's at several large companies.

Garretson, C. (2003, September 1). Under the gun. Network World, Vol. 20 Issue 35, p38, 2p

In this article Garretson discusses the concern of the United States Congress and California legislature regarding data security and information privacy and the regulatory policies that have resulted. The article focuses specifically on the impact of these regulations on corporate IT departments from a compliance and financial perspective. This article was published in Network Computing, a widely published and respected magazine that focused on network technology and the networking market. The author, Cara Garretson, is a Senior Editor at Network Computing Magazine and the Washington D.C. correspondent for the IDG News Service.

Data from this article are used in the Purpose and Problem Area sections to define the regulations companies face in protecting data and ensuring privacy. This resource is also used to define the scope of the problem and define the challenges that corporations face in meeting these new responsibilities.

Vijayan, J. (2003, October 6). Laws, Concern for Corporate Image Make Privacy A Priority. Computerworld; 10/6/2003, Vol. 37 Issue 40, p12, 3/4p

In this article Vijayan outlines the state and federal government regulations that have been created to protect the privacy and integrity of personal data. The author goes on to discuss high profile breaches of data security at companies and the consequences of these breaches to the company in general and to the companies' management in particular. The article also outlines risks and threats that exist for securing corporate networks and the level of importance of mitigating these risks with a security policy. The article was published in Computerworld, a leading technology publication focused on IT managers. The author, Jaikumar Vijayan, is a Senior Editor for Computerworld magazine.

This article is used in the Purpose section to describe the government regulations that define corporate responsibilities in protecting data and ensuring privacy and to outline the consequences of non-compliance. This resource is also used in the Problem Area section to define the risks and challenges that companies face in securing data networks and developing security policy.

References Related to Research Methodology

Krippendorff, K. (2004). *Content Analysis.* Thousand Oaks: Sage Publications Inc.

This text provides detailed information on the content analysis strategy. Topics covered in this text are the conceptual foundation for content analysis, the components of

content analysis, including unitizing and coding, research and analysis methods. The author of the text, Klaus Krippendorff, is a Professor at the University of Pennsylvania and a widely published author in the field of research methodology.

This reference is used in the Purpose and Method sections to define the research method and data analysis strategy used for the study. Specific areas referenced are the qualitative versus quantitative research, defining the type of analysis to use, formulating the research questions and defining the criteria for source selection.

Leedy, P. D., & Ormrod, J. E. (2001). *Practical Research Planning and Design.* Upper Saddle River: Prentiss-Hall Inc.

This book contains information on the planning and execution of a research effort. The authors define the research process by leading the reader through the process of (1) defining the research problem, (2) developing the design/strategy for obtaining data, (3) evaluating the data collected and (4) writing the research proposal. It also contains information on the both qualitative and quantitative research methodologies and how to apply these in the research process. This resource was chosen based upon the recommendation of the Professor Jane Gholson of the University of Oregon.

Data from this resource are used in the Purpose and Method sections to define the research methodology the researcher takes to obtain resources and analyze the content. Specific topics referenced were: qualitative research methodology, resources for performing a literature review and criteria for determining the validity of data obtained.

Palmquist, Mike, et al. (2005). Content Analysis. Writing@CSU. Colorado State University Department of English. Retrieved [Date] from http://writing.colostate.edu/references/research/content/.

This web site provides information on the process of conducting content analysis. It is structured to give the researcher a step-by-step means for understanding the process of performing a content analysis including conceptual analysis and relational analysis. This resource was chosen based upon its affiliation with the Colorado State University Writing Center.

This resource is used in the Purpose and Method sections to develop the data analysis process for the study. It is used to structure the eight coding steps in data analysis.

CHAPTER III - METHOD

The over arching research method used for this study is literature review (http://www.utoronto.ca/writing/litrev.html) of sources relating to wireless local area network technology as well as corporate security and privacy regulations. A conceptual analysis, as defined by the Colorado State University Writing Center (Palmquist et al., 2005) is then applied on the data collected to create a base of knowledge on the specifications, characteristics, capabilities, vulnerabilities and operability of the standards and protocols that represent the focus of the study.

The first stage in the research process is the formulation of research questions (Krippendorff, 2004, pg. 343-344). The goal of this initial step is to determine the over arching questions that need to be answered in order to successfully develop the study as well as begin the process of setting the context of the study. A top-down approach (Palmquist et al., 2005) is taken that begins with the definition of larger, primary, questions relating to the problem areas followed by successive, secondary, questions that define the problems in more specific terms. This process starts with the creation of the primary research question:

- What methods exist for securing wireless local area networks?

In the course of examining this question several more specific questions are developed to help frame the focus of the study. These are:

- What are the characteristics of the WLAN market?

- What standards define wireless local area networks?
- What means of security exist for WLAN's?
- What risks exist for companies when deploying WLAN's?
- What are the main concerns companies have when defining security policy?
- Who is responsible for developing corporate security policy? What challenges do they face? What consequences to they face?
- What are responsibilities do companies have in ensuring data security and privacy? What consequences companies do face if they do not meet their responsibilities?

These secondary questions define the framework for the study and serve as the foundation for the creation of the full purpose and for the remaining stages of the research process.

Data Collection

The second stage in the research process is to determine the criteria by which the literature is to be searched. The goal of this step is to transform the research questions defined in step one into a specific set of key words and phrases that represent the critical characteristics of the bodies of knowledge. (Krippendorff, 2004, pg. 345-347). As a first step in this process bodies of knowledge are defined based upon their relevance to the research questions and include: wireless local area network security protocols, wireless local area network security standards, wireless local area network security risks, wireless local area network market information and corporate data privacy regulations and responsibilities. The next step in the process is the development of a list of key words and

phrases based upon the bodies of knowledge defined in step one. This list is used to define the search metrics for the data collection stage.

The third stage of the research process is data collection. The purpose of this stage is to use the criteria defines in stage two to obtain references relating to the focus of the paper (Palmquist et al., 2005). The data collection process is executed in steps beginning with the definition of search queries. These queries are built using the list of key words and phrases and used as the foundation of the entire data collection strategy. Once defined, these queries are used as to access data from:

- The University of Oregon Online Library
    - Lexis-Nexis Academic
    - Business Source Premier
    - EconLit
- Internet Search Engines
    - Google
    - IEEE Archives
    - IETF Archives
- The Georgia Institute of Technology Library
    - Engineering Library
    - College of Management Library
- The Emory University Library
    - Goizueta School of Business Library
- IEEE technical reference CD's

These repositories are selected based upon their availability, size and ease of access. The first step in the strategy used to access data contained in these repositories consists of defining those repositories most likely to have data relating to the bodies of knowledge. For sources pertaining to business, market and privacy searches focused on the business libraries of The Georgia Institute of Technology, Emory University and the search engines of The University of Oregon Online Library. For technical information the primary source is The Georgia Institute of Technology Engineering library, the IEEE and IETF archives and Internet search engines. The second step in the data gathering process uses key words and phrases to build queries that define the parameters of the searches including, in some cases, publication, date of publication and author.

Once collected, the data are initially evaluated to determine usefulness. The criteria used to evaluate the data are consistency of the material, timeliness of the source and frequency of occurrence. Material deemed to be useful is then organized. In order to add a level of clarity and to facilitate the analysis process to follow the data is categorized based upon its relation to the following topics:

- Security
- Protocols
- Market
- Privacy
- Standards

These terms are selected because they represent the larger focus areas of the paper, specifically WLAN standards, WLAN security protocols, the WLAN market and corporate privacy. The goal of defining these categories is primarily organizational as this method facilitates the analysis by creating a structure for the sources based upon content, topic and relevance. Grouping the sources in this way also provides the foundation for the detailed analysis to follow by creating a common base of knowledge and a unified reference structure facilitating the processes of source referencing and information access.

Data Analysis

The final stage of research process is content analysis. This stage takes a qualitative approach to analyzing the data gathered (Krippendorff, 2004, pg. 87-89) by applying the eight steps of conceptual analysis as defined by the Colorado State University Writing Center (Palmquist et al., 2005).

In the first step of the process, the level of analysis is defined to code for a specific set of pre-determined phrases and terms. This decision stems from the definition of key terms and the need for complex search queries. The specific phrases and terms used for this step are summarized in Table 1: Key Search Terms & Phrases.

Key Phrases	Key Terms
WLAN Security	802.11
WLAN Standard	802.11i
WLAN Protocol	802.1x
Key Management	Wi-Fi Alliance
Key Rotation	PKI
EAP-TLS Characteristics	SSID

Key Phrases	Key Terms
WPA Characteristics	MIC
WEP Characteristics	TKIP
EAP-TLS Vulnerabilities	RC4
WPA Vulnerabilities	Encryption
WEP Vulnerabilities	Authentication
Digital Certificate	RADIUS
Centralized Authentication	AES
Decentralized Authentication	RSN

Table 1: Key Search Terms & Phrases

The second stage of the process defines the number of phrases and terms to code for and this is also accomplished by referencing the list of key terms and phrases outlined in table one. Next the key terms and phrases are applied to the reading of the references, with each reference annotated according to the occurrence of each term, or phrase, as they appears in the text. The coding process is accomplished by first electronically parsing through the reference marking all places where a key phrase of term appears. In the next step the researcher reads through the sources and, where the text has been marked, adds details on what is covered. The final step is for the researcher to eliminate the data that are not specific enough or do not address the key search topics and then electronically highlight and categorize, the remaining text for future reference. It is important to note that although the list of key terms and phrases is pre-defined in very specific terms, some latitude is given in coding in order to allow for like terms with the same meaning to be included. This step allows the researcher to define specific guidelines for analysis, resulting in a base of data focused on specific topics. This step also facilitates the process of eliminating weak and irrelevant data, ensuring the validity and relevance of the data.

The final step in the process is to review the coded and categorized results as a means to draw pertinent information from them. This is accomplished first by re-categorizing each of the selected references in relation to (1) WLAN Security Protocol Capabilities, (2) WLAN Security Protocol Vulnerabilities, or (3) WLAN Security Protocol Components. Once categorized according to these three major headings, the data is analyzed and presented in four tables. The first table (see Table 6) defines each of the three protocols in terms of the encryption, authentication and key management capabilities. The second table (see Table 7) presents the vulnerabilities that exist in the encryption, authentication and key management capabilities of each of the three protocols. The third table (see Table 8) shows the specific encryption, authentication and key management components of each of the three protocols. The presentation of each of these tables is followed by an explication of the meaning of the data in terms of the key ideas, framed for the audience. A fourth table (see Table 5) demonstrates the relationship of each of the three protocols to the standard in which they are defined.

Data Presentation

The outcome of the research process presents the results of the content analysis, framed for IT executives, in the form of (1) an annotated bibliography of published sources relating to the focus areas of the study and (2) an aggregated table showing the capabilities of the three protocols analyzed with respect to the criteria defined in the 802.11i standard.

Selected, sources are organized by their relevance to the categories of security, protocols, market, privacy and standards and presented in an annotated bibliography. Annotations provide the audience, i.e., IT executives responsible for developing corporate security policy, with a logical and structured means of obtaining greater information and insight into the research elements of the study as well as providing a reference for future study. The second outcome is a table (see Table 2: Wireless Security Protocol Reference Table) that provides a visual representation of the three selected wireless local area network security protocols (WEP, WPA and EAP-TLS) based upon their compliance to the criteria specified in the IEEE 802.11i, specifically, their capabilities in the areas of authentication, encryption and key management as defined in the IEEE 802.11i standard. A template of the table is presented below (see Table 2).

Table 2: Template - Wireless Security Protocol Reference Table

		Criteria		
Standard	Protocol	Authentication	Encryption	Key Management
802.11	WEP	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:
Wi-Fi Alliance	WPA	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:
802.1X	EAP-TLS	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:	Method: Benefits: Vulnerabilities: Limitations:

The goal of this table is to provide a summary overview of the results of the content analysis, enabling a side-by-side comparative analysis of the definitions, specifications, characteristics, capabilities, vulnerabilities and operability of the protocols studies based upon the criteria defined in the IEEE 802.11i protocol. The researcher intends that IT executives responsible for developing corporate security policy can use these two outcomes as references when determining corporate security policy.

CHAPTER IV – ANALYSIS OF DATA

This chapter is a report of the content analysis conducted to define the capabilities, vulnerabilities and components of the WEP, WPA and EAP-TLS protocols. Thirty-eight sources are analyzed, outlined in Appendix B Table 3: Sources Used In Content Analysis.

Stage One of Content Analysis: Definition of Coding Terms and Phrases

In the coding phase the key terms and phrases defined in Table 4 are used to review the references. In order to ensure the proper level of analysis is performed, these key terms and phrases are also combined making complex phrases as a method for defining the characteristics of the protocol studies. These terms represent a sub-set of the key terms and phrases table defined in the method section and are selected because they focus on those terms and phrases pertaining to WLAN security standards and protocols. This table of terms and phrases is defined in Table 4: Data Analysis Coding Terms and Phrases.

Key Phrases	Key Terms
WLAN Security	802.11
WLAN Standard	802.11i
WLAN Protocol	802.1x
Key Management	Wi-Fi Alliance
Key Rotation	PKI
EAP-TLS Characteristics	SSID
WPA Characteristics	MIC
WEP Characteristics	TKIP
EAP-TLS Vulnerabilities	RC4
WPA Vulnerabilities	Encryption
WEP Vulnerabilities	Authentication

Key Phrases	Key Terms
Digital Certificate	RADIUS
Centralized Authentication	AES
Decentralized Authentication	RSN

Table 4: Data Analysis Coding Terms and Phrases

Stage Two of Content Analysis: Coding Selected Literature

In this stage of the process the references defined in Table 3: Sources Used In Content Analysis are read and coded according to the terms and phrases listed in Table 4: Data Analysis Coding Terms and Phrases. This coding process is a critical step in the study as it extracts data from the resources upon which a body of knowledge can be built that defines the capabilities, vulnerabilities and components of the WEP, WPA and EAP-TLS protocols. This step also makes certain that these capabilities, vulnerabilities and components are consistent, repeatable and cited ensuring their reliability and validity. It is important to note that the existence of a key term or phrase in a source does not constitute its inclusion into the body of knowledge. Prior to inclusion, all capabilities, vulnerabilities and components must be referenced multiple times in different sources and be consistent, cited and supported by data.

The next step in the coding stage is to organize the data that results from the coding phase of the content analysis by placing the annotated references into specific categories from which comparisons can be made, inconsistent data eliminated and conclusions drawn. The results are represented in tabular form based upon their relationship to the following categories:

- WLAN Security Protocol Capabilities (see Table 6)
- WLAN Security Protocol Vulnerabilities (see Table 7)
- WLAN Security Protocol Components (see Table 8)

Stage Three of Content Analysis: Presentation of Coding Results

Results from the first step of the analysis are presented in Table 5: Data Related To WLAN Security Standards. This table presents the security methods defined by the four standards as well as the number of references that are used to build this table. Also included in this table is the IEEE 802.11i standard that serves as the criteria of the study. Coding terms and phrases used in this part of the analysis are 802.11, 802.11i, 802.1x, Wi-Fi Alliance.

WLAN Standard	Security Protocol	Frequency
IEEE 802.11	Wired Equivalent Privacy (WEP)	7
IEEE 802.1x	EAP-TLS	10
Wi-Fi Alliance	Wi-Fi Protected Access (WPA)	8
IEEE 802.11i	Robust Security Network (RSN)	10

Table 5: Data Related To WLAN Security Standards

This portion of the process validates the existence of a security method in each of the standards that define the purpose of the study. A frequency element is also included in this table to show the number of sources identified, relating to each of these standards, as a means of legitimizing the amount of data that exists on these topics relative to the data set used in the Analysis of Data chapter.

Results from the second step of the analysis are presented in Table 6 and define the capabilities of the WLAN security protocols in relation to encryption, authentication and key management. As defined in the Definition section (see Appendix A) Encryption refers to "Any procedure used in cryptography to convert plaintext into ciphertext in order to prevent any but the intended recipient from reading that data". Authentication refers to "A mechanism that allows the receiver of an electronic transmission to verify the sender and the integrity of the content of the transmission through the use of an electronic key or algorithm, which is shared by the trading partners." And key management refers to "A process by which key is generated, stored, protected, transferred, loaded, used, and destroyed". Defining these terms in the proper context is critical to the execution of this chapter as they represent the foundation, and criteria, for the study.

Coding terms and phrases used in this part of the analysis are WEP Characteristics, WPA Characteristics, EAP-TLS Characteristics, Authentication, Encryption, Key Management, Key Rotation, Centralized Authentication, Decentralized Authentication, and Digital Certificate. This data is important as it directly defines the level, or levels, of security the protocols are able to support or not support.

Security Protocol	Encryption	Authentication	Key Management
WEP	• 40-bit key/28-bit hash • Static keys	• Shared Key • Open system	• Manual Key Rotation
WPA	• 128-bit key/48-bit hash • Constant Key Rotation	• Centralized authentication • Decentralized authentication • Digital Certificates	• Per packet key rotation

Security Protocol	Encryption	Authentication	Key Management
		• Shared Key	
EAP-TLS	• 128-bit keys • Constant Key Rotation	• Centralized authentication • Decentralized authentication • Digital Certificates	• Per session key rotation

Table 6: Data Related To WLAN Security Protocol Capabilities

Table 6 reveals the capabilities of each of the protocols both in individual terms and in comparison to each other in relation to:

- The different levels of encryption data hashing
- The flexibility of each protocol in regards to authentication
- The degree of key management available

As shown, Table 6 allows for direct comparison of the protocols capabilities in terms of level of functionality. Key points of information revealed in this data are:

- *The increase in encryption key length between EAP-TLS, WPA, and WEP.* The length of the encryption key is directly related to the ability of the messages to remain secure with longer keys allowing for greater security by making decoding more complicated.
- *The additional options that exist for authentication with WPA and EAP-TLS as opposed to WEP.* Specifically the ability of WPA and EAP-TLS to support both centralized and decentralized user authentication provides greater flexibility by allowing large organizations to implement a centralized authentication process with the ability to support larger user bases. Smaller organizations are also allowed to implement a decentralized solution, which can be implemented and supported at a lower cost.

- *The lack of key rotation capabilities for WEP.* There is no defined method for the distribution, or rotation, of encryption keys in the IEEE 802.11 WEP standard leaving manual rotation as the only option.

Results from the third step of the analysis are presented in Table 7: Data Related to WLAN Security Protocol Vulnerabilities. Coding terms and phrases used in this part of the analysis are WEP Vulnerabilities, WPA Vulnerabilities, EAP-TLS Vulnerabilities, Authentication, Encryption and Key Management. Data in this table highlights the security exposures associated with each of the three examined security protocols.

Security Protocol	Encryption	Authentication	Key Management
WEP	• Static encryption key • RC4 algorithm decodable • Hash value reused	• No user-level authentication • 40-bit shared key decodable • Insufficient message integrity checking	• Manual key rotation
WPA	• Dictionary attacks • RC4 algorithm decodable	• Pre-shared key decoding	• None
EAP-TLS	• Static hash key • Open key exchange	• Device-based authentication only • Unilateral authentication	• None

Table 7: Data Related To WLAN Security Protocol Vulnerabilities

Table 7 reveals the vulnerabilities of each of the protocols in relation to:

- The differing degrees of severity

- The number of vulnerabilities that exist for each protocol
- Common problems that exits across protocols

As shown, Table 7 allows for direct comparison of vulnerabilities in terms of their risks to security and/or lack of functionality. Key points of information revealed in this data are:

- *The ability of the RC4 encryption protocol to be decoded.* As the algorithm that provides the means to encrypt data for WEP and WPA, this vulnerability allows non-trusted persons to decode the encryption key by capturing data packets. This is of particular importance in the WEP protocol as the encryption keys are not rotated automatically.
- *Device based authentication in the EAP-TLS protocol.* The EAP-TLS protocol authenticates devices instead of users. This authentication method presents the risk of captured devices (i.e. equipment belonging to a trusted user that is in the possession of a non-trusted user) to communicate over the network without verifying the actual operator.
- *The lack of key management vulnerabilities found for WPA and EAP-TLS.* Not a single documented key management vulnerability could be found for WPA or EAP-TLS. This can be seen as an indicator of the strength and reliability of these capabilities.

Results from the final step of the analysis are presented in Table 8: Data Related to WLAN Security Protocol Components. Each protocol is examined in relation to three components: encryption, authentication and key management. These components

represent the specific, programmatic, functions of the protocols. Coding terms and phrases used in this part of the analysis are PKI, SSID, MIC, TKIP, RC4, RADIUS, AES, RSN, Authentication, Encryption and Key Management.

Security Protocol	Encryption	Authentication	Key Management
WEP	• RC4 (24-bit hash)	• SSID • Pre Shared Key	• None
WPA	• TKIP (w/ RC4) • AES	• RADIUS • EAP • PKI	• TKIP
EAP-TLS	• TLS	• EAP • RADIUS • PKI	• TLS

Table 8: Data Related To WLAN Security Protocol Components.

Table 8 reveals the components of each of the WLAN security protocols in relation to:

- Components common to multiple protocols
- The number of encryption components each protocol supports
- The number of authentication components each protocol supports

As shown, Table 8 allows for direct comparison of the protocols vulnerabilities in terms of the specific components. Key points of information revealed in this data are:

- *The single option that exists for encryption with WEP and EAP-TLS.* This lack of options becomes important to organizations in the event these components become unstable or unsecured.
- *The ability of the TLS and TKIP components to support multiple security tasks.* On the positive side, these more functional components decrease the overhead on

the network for supporting these functions. On the negative side, more functional components may also increase the risk of impact of bugs or vulnerabilities.

- *The absence of a key management component for WEP.* No method for key management means that encryption key rotation requires manual intervention, which increases the time and cost for management and raises the risk of encryption key decoding the longer the keys are not rotated.

The results for the data analysis process provide a multi-dimensional representation of the WEP, WPA and EAP-TLS protocols that define the purpose of this study. Considered individually, Tables 6, 7 and 8 provide a one-dimensional view of the protocols, which is not adequate for defining the protocols benefits, risks and usability. However, the tables provide a data-rich foundation for the discussion of these protocols, presented in the Conclusions chapter of this paper. Conclusions examine the functional parameters of the protocols and note the key information that this data revealed, framed for IT executives with responsibility for defining corporate data security.

CHAPTER V – CONCLUSIONS

At the conclusion of this study it is important to reiterate that the purpose is not to define for the audience the proper WLAN security protocol to use, but rather to provide a comprehensive representation of the capabilities, vulnerabilities and components of the WEP, WPA and EAP-TLS protocols. The goal is to present in this information in such a way that IT Executives responsible for wireless security can understand, and apply, these protocols in their organizations.

Presentation of the Wireless Security Protocol Reference Table

Table 2: Wireless Security Protocol Reference Table, presented below, encapsulates the data presented in the Analysis of Data chapter into a master table. Table 9 is designed to show the capabilities, vulnerabilities and components of the three protocols (WEP, WPA and EAP-TLS), each in relation to three basic criteria: (1) authentication, (2) encryption and (3) key management. The purpose of this table is to provide a comprehensive and comparative reference that IT executives responsible for wireless security can use in the development of corporate security policy.

Table 9: Wireless Security Protocol Reference Table

		CRITERIA		
Standard	**Protocol**	**Authentication**	**Encryption**	**Key Management**
802.11	WEP	**Capabilities:** • Shared Key • Open system **Vulnerabilities**: • No user-level authentication • 40-bit shared key decodable • Insufficient message integrity checking **Components**: • SSID • Pre Shared Key	**Capabilities**: • 40-bit key/28-bit hash • Static keys **Vulnerabilities**: • Static encryption key • RC4 algorithm decodable • Hash value reused **Components**: • RC4 (24-bit hash)	**Capabilities**: • Manual Key Rotation **Vulnerabilities:** • Manual key rotation **Components**: • None
Wi-Fi Alliance	WPA	**Capabilities**: • Centralized authentication • Decentralized authentication • Digital Certificates • Shared Key **Vulnerabilities**: • Pre-shared key decoding **Components**: • RADIUS (Centralized) • EAP (Decentralized) • PKI	**Capabilities**: • 128-bit key/48-bit hash • Constant Key Rotation **Vulnerabilities**: • Dictionary attacks • RC4 algorithm decodable **Components**: • TKIP (w/ RC4) • AES	**Capabilities**: • Per packet key rotation **Vulnerabilities**: • None **Components**: • TKIP

		CRITERIA		
802.1X	EAP-TLS	**Capabilities**: • Centralized authentication • Decentralized authentication • Digital Certificates **Vulnerabilities**: • Device-based authentication only • Unilateral authentication **Components**: • EAP • RADIUS • PKI	**Capabilities**: • 128-bit keys • Constant Key Rotation **Vulnerabilities**: • Static hash key • Open key exchange **Components**: • TLS	**Capabilities**: • Per session key rotation **Vulnerabilities**: • None **Components**: • TLS

Interpretive Key for Review of Elements in Table 2

The study concludes with an amplified discussion of each of the elements presented in Table 9: Wireless Security Protocol Reference Table, and is designed for use by IT executives as an interpretive key when working with the table. The key consists of further discussion of the capabilities, vulnerabilities and components of each of three basic criteria: (1) authentication, (2) encryption and (3) key management – in relation to the three selected standards and protocols. While information is presented for each element in Table 9, those elements that appear under multiple protocols, or that are functionally identical in their implementations, are included only once.

Discussion of *Authentication Capabilities*

Within the 802.11 standard and WEP protocol:

- ***Shared Key Authentication:*** Shared key authentication is a process by which WLAN clients are provided network access based upon their response to a challenge by the authenticating access point (Chandra, 2002; Shinder,2004). The method of authentication, referred to as challenge-response (Chandra, 2002), is the exchange of an identical numerical value (Chandra, 2002; Shinder, 2004; DeBeasi, 2004) that is configured on both the requestor (client) and authenticator (access point). This numerical value is used by the authenticator to validate client permissions and grant/deny access. (Geier, 2003; Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005)
- ***Open System Authentication:*** Open system authentication provides access to any requestor based upon a successful transmission of an alphanumeric value called a service set identifier (Balinsky & Miller & Sankar & Sundaralingam, 2005). This value is used by the access point to validate client permissions and grant/deny access (Chandra, 2002; Arbaugh & Edney, 2004).

Within the Wi-Fi Alliance and 802.1X standards and the WPA and EAP-TLS protocols:

- ***Centralized Authentication:*** This method of device authentication uses a central server to validate client permissions and grant/deny access (Molta, 2002; Pabrai & Uday, 2004; Roshan, 2001; Roberts, 2003). In this method, client requests are

forwarded on to the central server at the access point, which holds responsibility to grant/deny (Snyder & Thayer, 2004; Welcher, 2004; Wildstrom, 2002.).

- ***Decentralized Authentication:*** Decentralized authentication assigns client authentication to the access points by using pre-shared keys (Shinder, 2004; Arbaugh & Edney, 2004). However, this method differs from share key authentication in that the pre-shared keys are periodically rotated based upon the authentication algorithm used (Snyder & Thayer, 2004; Shinder, 2004).
- ***Digital Certificates:*** Digital certificates are electronic messages that contain security values used to validate client permissions (Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005, pg. 31-32). In authentication methods where digital certificates are used both the client (requestor) and server (authenticator) must have identical certificate values to communicate (Dornan, 2004; Halasz, 2004; Molta, 2002; Snyder & Thayer, 2004; Welcher, 2004).

Discussion of *Encryption Capabilities*

Within the 802.11 standard, WEP Protocol:

- ***40-bit key/28-bit hash:*** A 40-bit key, with a 28-bit hash, is a numeric value used by devices on a wireless local area network to encrypt and decrypt data. This value must be known by the clients at each end of the conversation in order for the data to be understood (Pabrai & Uday, 2004; Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005).

- ***Static keys:*** Static keys are numeric values used for the encryption and decryption of data that are manually defined and cannot be changed on an ad-hoc basis or via an automated process. (Steinke, 2002; Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005).

Within Wi-Fi Alliance standard and WPA protocol:

- ***128-bit key/48-bit hash:*** A 128-bit key, with a 48-bit hash, is a numeric value used by devices on a wireless local area network to encrypt and decrypt data. This value must be known by the clients at each end of the conversation in order for the data to be understood (Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005). In contrast to a 40-bit key/28-bit hash key, these values are more sophisticated in their ability to encrypt data and as such more difficult to compromise (Huckaby, 2001; Arbaugh & Edney, 2004).
- ***Constant Key Rotation:*** This method of data encryption automatically changes the encryption value/key at defined intervals. This method of encryption can be contrasted to static keys, which use the same value/key for all clients with automated process for key rotation (Arbaugh & Edney, 2004, pg. 243-244; Omatseye, 2003; Passmore, 2004; Shinder, 2004; Wikipedia, 2005).

Discussion of *Key Management Capabilities*

Within the 802.11 standard, WEP Protocol:

- ***Manual Key Rotation:*** Manual key rotation rotates encryption keys by means of human manual intervention. This process can take many forms but must be

accomplished by a person gaining physical or remote access to each device (Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005; Chandra, 2002)

Within the Wi-Fi standard, WPA protocol:

- ***Per packet key rotation:*** This method of key management creates a new encryption key each time a packet is communicated between clients. (Passmore, 2004; Snyder & Thayer, 2004; Arbaugh & Edney, 2004, pg. 243-244; Shinder, 2004)

Within the 802.1X standard, EAP-TLS protocol:

- ***Per session key rotation:*** Per session key rotation changes the encryption key each time a new session is created between clients. A derivative of per session key rotation is timed key rotation whereby the encryption key is changes at regularly defined intervals (Geier, 2003; Ou, 2002; Arbaugh & Edney, 2004.)

Discussion of *Authentication Vulnerabilities*

Within the 802.11 standard, WEP protocol:

- ***40-bit Shared Key decodable:*** The standard 40-bit key authentication method have proven to be easily decodable via packet capture and analysis exposing companies to risks including man in the middle attacks, denial of service attacks and session hijacking (Chandra, 2002; DeBeasi, 2004; Disabato, 2003; Halasz, 2004; Passmore, 2004; Steinke, 2002). This vulnerability has been confirmed by

organizations including The University of California-Berkley, The Weizman Institute and Cisco Systems (Gain, 2001; Albright, 2003).

Within Wi-Fi standard, WPA protocol:

- ***Pre-shared key decodable:*** The problems that exist related to pre-shared keys focuses on the use of short session keys and pass phrases (Roberts, 2003). Like the problems that exist with the 40-bit shared key this vulnerability allows intruders to capture and analyze packets until they are able to decipher the key. With this key the intruder can execute a dictionary attack on the network until the pass phrase is guessed (Roberts, 2003; Snyder & Thayer, 2004)

- ***Insufficient message integrity checking:*** This vulnerability focuses on the use of Cyclic Redundancy Check (CRC) as the means of ensuring data integrity (Chandra, 2002; DeBeasi, 2004; Steinke, 2002). The problem with this is that CRC does not use a cryptographic key instead transmitting data in clear-text allowing intruders to alter the data in the packets (Chandra, 2002; Steinke, 2002).
- ***Unilateral authentication /Device-based authentication only/ No user-level authentication:*** These three items represent the same fundamental authentication problem. Unilateral authentication validates clients based upon the devices configuration but does not validate the person using it. This presents the risk of device hijacking and the introduction of rogue access points. (Connolly, 2002; Dornan, 2004; Chandra, 2002)

Discussion of *Encryption Vulnerabilities*

Within the 802.11 standard and WEP protocol:

- ***Static encryption key:*** Static encryption keys represent a vulnerability to WLAN's base due to their inability to change the key in an automated fashion. The real threat to organizations is that once compromised the static keys can be used by an intruder to access the network unobstructed. In addition, once compromised, static keys must be changed manually increasing the time it takes to re-secure the network (Andress, 2002; DeBeasi, 2004; Disabato, 2003; Ou, 2002).

Within the 802.11 and Wi-Fi Alliance standards and the WEP and WPA protocols:

- ***RC4 algorithm decodable:*** The RC4 algorithm has been found to be generally unsecure (Arbaugh & Edney, 2004; Wildstrom, 2002) and susceptible to decoding via packet capture and analysis tools. The risks this poses to organizations includes an in the middle attacks, denial of service attacks and session hijacking (DeBeasi, 2004; Halasz, 2004; Molta, 2002; Mooney, 2002; Steinke, 2002).

Within the 802.1X standard and EAP-TLS protocol:

- ***Static hash key/ Hash value reused:*** This vulnerability deals with the reuse of the value used to encrypt data (Dornan, 2004). For the protocols that utilize this type of data hashing the risk exists for an intruder to capture and analyze the packets then using a dictionary attack approach to decipher that hash (Dornan, 2004). If

the intruder is successful in breaking the hash they will be able to decipher all encrypted traffic transmitted across the WLAN.

Discussion of *Key Management Vulnerabilities*

Within the 802.11 standard and WEP protocol:

- ***Manual key rotation:*** This vulnerability is directly related to the use of static encryption keys and deals with the risks associated with having to manually maintain and manage these static encryption keys (Chandra, 2002; DeBeasi, 2004). For organizations that employ a protocol that requires manual key rotation the problems include administrative overhead, increased risk of the key being compromised and a decreased ability to react to and close security breeches. (Geier, 2003; Mooney, 2002; Steinke, 2002)

Discussion of *Authentication Components*

Within the 802.11 standard and WEP protocol:

- ***SSID (Service Set Identifier):*** The Service Set Identifier, or SSID, is "an alphanumeric code configured on both the wireless NIC and the access point an alphanumeric code" (Pabrai & Uday, 2004) that is used by the access point to validate client permissions and grant/deny access (DeBeasi, 2004; Molta, 2002). SSID's are broadcast unencrypted by default but this functionality can be suppressed via configuration changes (Molta, 2002; Steinke, 2002). SSID's must be manually configured on all access points.

Within the Wi-Fi Alliance and 802.1X standards and the WPA and EAP-TLS protocols:

- ***PKI (Public Key Infrastructure):*** PKI is an authentication method where each device on the WLAN contains a unique key, contained in a digital certificate, (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html) that is used when requesting network access. The authentication server uses this key to positively identify the device. PKI keys can be revoked if lost, stolen or compromised. (Dornan, 2004; Nelson, 2004; Mooney, 2002). The use of PKI requires a centralized authentication infrastructure.

- ***RADIUS (Remote Authentication Dial-In User Service):*** RADIUS is a challenge/response protocol that provides centralized device authentication via the validation of a username and password (Ou, 2002; Shinder, 2004). RADIUS requires the use of a dedicated server that all client authentication requests are forwarded to and that contains the master database of all client credentials (Snyder & Thayer, 2004; Welcher, 2004).

- ***EAP (Extensible Authentication Protocol):*** EAP is an authentication protocol that defines a framework for device authentication across wired and wireless networks. EAP is centered on providing authentication via the use of secure keys (Pabrai & Uday, 2004; Snyder & Thayer, 2004; Welcher, 2004). Its strength is in its ability to support multiple authentication methods including passwords, digital certificates and public-keys (Geier, 2003;

www.sofweb.vic.edu.au/ict/lan/wireless_glossary.htm; Connolly, 2002; Dornan, 2004; Roshan, 2001)

Discussion of *Encryption Components*

Within the 802.11 and Wi-Fi Alliance standards and the WEP and WPA protocols:

- ***RC4:*** RC4 is a computer algorithm that encrypts data by altering the input text using a random permutation (http://www.techuser.net/randpermgen.html) method. RC4 is the most common, and widely used, encryption algorithm used in wireless LAN communications (Chandra, 2002; DeBeasi, 2004; Molta, 2002; Shinder, 2004; Steinke, 2002).

Within the Wi-Fi Alliance standard and WPA protocol:

- ***TKIP (Temporal Key Integrity Protocol):*** TKIP is a data encryption protocol that uses the RC4 algorithm as its underlying cipher method (Omatseye, 2003; Wildstrom, 2002). However, TKIP enhances RC4 by providing per packet encryption key rotation to ensure data integrity, message integrity checking (MIC) and a longer initialization vector (http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci887323,00.html; Wikipedia, 2005; Shinder, 2004; Snyder & Thayer, 2004; Halasz, 2004).

- ***AES (Advanced Encryption Standard):*** AES is a data encryption algorithm that supports up to 256-bit keys and uses a block cipher method to encrypt data (Shinder, 2004; Garcia, 2005). While this method on data encryption is

considered extremely secure (Mooney, 2002; Cohen & O'Hara, 2003; Shinder, 2004) a potential downside is that because of the sophistication of the AES algorithm some legacy wireless devices may require hardware and software upgrades in order to support it (Chandra, 2002; Huckaby, 2001; Griffith, 2004). AES is also the standard method for encryption for the United States Government (Shinder, 2004; Griffith, 2004; Funk, 2005).

Within the 802.1X standard and EAP-TLS protocol:

- ***TLS (Transport Layer Security):*** TLS is an authentication and security protocol that uses two separate protocols to negotiate connectivity and ensure data encryption (Dornan, 2004; Arbaugh & Edney, 2004). At the center of TLS are digital certificates that identify the individual clients, pass user authentication fields and generate public-and-private encryption keys. TLS is defined in IETF RFC-2246 as the standardized version of the Secure Sockets Layer (SSL) encryption protocol. (Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005; Chandra, 2002)

Discussion of *Key Management Components*

Within the Wi-Fi Alliance standard and WPA protocol:

- ***TKIP (Temporal Key Integrity Protocol):*** The TKIP protocol provides per-packet encryption key rotation (Snyder & Thayer, 2004; Halasz, 2004; Shinder, 2004). This means that each time a packet is transmitted between clients that key used to encrypt and decrypt the data is changed to a new, randomly selected, value (DeBeasi, 2004; Wikipedia; 2005). This method of key management greatly reduces the risk of dictionary and man-in-the-middle attacks (Cohen & O'Hara, 2003; Griffith, 2004; Pabrai & Uday, 2004; Robinson, 2004).

Within the 802.1X standard and EAP-TLS protocol:

- ***TLS (Transport Layer Security):*** The TLS protocol provides per-session encryption key rotation (Dornan, 2004; Geier, 2003). Per-session key rotation changes the encryption key each time a new client-to-client session is established. This method of key management greatly reduces the risk of dictionary and man-in-the-middle attacks. (Arbaugh & Edney, 2004; Balinsky & Miller & Sankar & Sundaralingam, 2005; Chandra, 2002)

APPENDIX A

Definitions

802.11: "802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997" (http://www.webopedia.com/TERM/8/802_11.html)

802.11b: "An extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet" (http://www.webopedia.com/TERM/8/802_11.html)

802.11i: "802.11i is a standard for wireless local area networks (WLANs) that provides improved encryption for networks that use the popular 802.11a, 802.11b (which includes Wi-Fi, and 802.11g standards. The amendment adds stronger encryption, authentication, and key management strategies that go a long way toward guaranteeing data and system security" (Halasz, 2004)

AES (Advanced Encryption Standard): "A federal information-coding protocol that ensures privacy via 128-, 192-, and 256-bit keys. AES is part of the 802.11i specification" (WLAN lingo, PC Magazine)

Algorithm: "A mathematical function that is used to encrypt and decrypt information." (www.pki.vt.edu/pki/glossary.html)

Authentication: “A mechanism that allows the receiver of an electronic transmission to verify the sender and the integrity of the content of the transmission through the use of an electronic key or algorithm, which is shared by the trading partners.” (usnet03.uc-council.org/glossary/)

BLOG: “A short form for weblog, a personal journal published on the Web. Blogs frequently include philosophical reflections, opinions on the Internet and social issues, and provide a "log" of the author's favorite web links” (www.fkcc.edu/links/library/lis2004/glossary.htm)

Capability: "The ability to execute a specified course of action." (www.globalsecurity.org/military/library/policy/army/fm/3-06/gloss.htm)

Component: "A reusable object or program that performs a specific function and is designed to work with other components and applications." (www.sabc.co.za/manual/ibm/9agloss.htm)

Content Analysis: “A research technique for making replicable and valid inferences from texts (or other meaningful matter) to the contexts of their use” (Krippendorff, 2004, pg. 18)

Denial of Service: " A hacker attack designed to shut down or overwhelm a system." (www.dis.wa.gov/portfolio/Definitions.htm)

Dictionary Attack: A brute force attempt to decrypt encrypted data by guessing passwords or pass phrases sequentially from a store of possible solutions. (www.cryptnet.net/fdp/crypto/crypto-dict.html)

Digital Certificate: “An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is

who he or she claims to be, and to provide the receiver with the means to encode a reply." (http://www.webopedia.com/TERM/D/digital_certificate.html)

EAP (Extensible Authentication Protocol): "EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards" (WLAN lingo, PC Magazine)

Encryption: "Any procedure used in cryptography to convert plaintext into ciphertext in order to prevent any but the intended recipient from reading that data" (www.pki.vt.edu/pki/glossary.html)

Hash: "A mathematical computation that takes a variable-size message and returns a fixed-size string to authenticate (prove the integrity) of a message." (www.sequi.com/SEQUI_VPN_Glossary.htm)

IEEE (Institute of Electrical and Electronics Engineers): "An organization that sets computing and communications standards, including all 802.11 standards" (WLAN lingo, PC Magazine)

IETF (Internet Engineering Task Force): "The main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual" (http://isp.webopedia.com/TERM/I/IETF.html)

Key Management: "A process by which key is generated, stored, protected, transferred, loaded, used, and destroyed" (www.jproc.ca/crypto/terms.html)

Man in the middle Attack: "An attack wherein attacker abuses weak or non-existent authentication mechanisms between two endpoints. By inserting himself between these endpoints, the attacker can not only view information passing back and forth, but can even modify or inject data going into such a connection." (http://business.cisco.com/glossary/tree.taf-asset_id=92882&word=103829&public_view=true&kbns=2&DefMode=.htm)

Message Integrity Code (MIC): Also referred to as a cryptographic checksum, a MIC is "a mathematical value (called a checksum) that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed" (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci869866,00.html)

Packet: "A packet is the fundamental unit of information carriage in all modern computer networks." (en.wikipedia.org/wiki/Packet)

Privacy: "Freedom from unauthorized intrusion" (http://www.m-w.com/cgi bin/dictionary?book=Dictionary&va=privacy)

Public Key Infrastructure (PKI): "A method for authenticating a message sender or encrypting a message. It enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. It provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates." (webdomino1.oecd.org/COMNET/PUM/egovproweb.nsf/viewHtml/index/$FILE/glossary.htm)

RADIUS (Remote Authentication Dial In User Service): "A protocol for remote user authentication and accounting. RADIUS enables centralized management of authentication data, such as usernames and passwords" (WLAN lingo, PC Magazine)

RC4: "An encryption algorithm designed at RSA Laboratories; specifically, a stream cipher of pseudo-random bytes that is used in WEP encryption" (support.intel.com/support/wireless/wlan/pro2200bg/userguide81/glossary.htm)

Regulation: "A rule or order issued by an executive authority or regulatory agency of a government and having the force of law" (http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=Regulation&x=18&y=8)

RSN (Robust Secure Network): "A protocol for establishing secure communications over an 802.11 wireless network. RSN (Robust Secure Network) is part of the 802.11i standard" (WLAN lingo, PC Magazine)

SSID (Service Set Identifier): "A code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a maximum of 32 alphanumeric characters. All wireless devices attempting to communicate with each other must share the same SSID" (en.wikipedia.org/wiki/SSID)

TKIP (Temporal Key Integrity Protocol): "The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs" (WLAN lingo, PC Magazine)

TLS (Transport Layer Security): "A protocol intended to secure and authenticate communications across a public networks by using data encryption. TLS is designed as a successor to SSL and uses the same cryptographic methods but supports more cryptographic algorithms" (http://www.cryptomathic.com/labs/techdict.html#t)

Vulnerability: A "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited." (www.keybank.com/html/A-11.2.1.html)

WEP (Wired Equivalent Privacy): "Part of the IEEE 802.11 standard (ratified in September 1999), and is a scheme used to secure wireless networks (WiFi). WEP was designed to provide comparable confidentiality to a traditional wired network" (http://www.netstumbler.com/faqs/dictionary/wep/)

Wi-Fi Alliance: "A nonprofit international association formed in 1999 to certify the interoperability of wireless LAN products based on the 802.11 specifications" (http://wi-fiplanet.webopedia.com/TERM/w/Wi_Fi_Alliance.html)

WLAN (Wireless Local Area Network): "A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes" (http://www.webopedia.com/TERM/W/WLAN.html)

WPA (Wi-Fi Protected Access): "A system to secure wireless (Wi-Fi) networks, created to patch the security of the previous system, WEP" (http://www.netstumbler.com/faqs/dictionary/wpa/)

APPENDIX B

Sources Used in Content Analysis

Table 3: Sources Used In Content Analysis.

Source	Topic Area
Andress, M. (2002, January 7). 802.11 wireless LANs. InfoWorld, Vol. 24 Issue 1, p36, 1/3p	• WEP vulnerability-authentication decode • WEP vulnerability-encryption
Anonymous (2003, November). Minimize the risk of wireless exposure. Communications News, Vol. 40 Issue 11, p32, 2p	• WEP vulnerability-authentication • WEP vulnerability-key management
Arbaugh, W. A., & Edney, J. (2004). *Real 802.11 Security.* Boston: Pearson Education Inc.	• Standards
Balinsky, A., & Miller, D., & Sankar, K., & Sundaralingam, S, (2005). Cisco Wireless LAN Security. Indianapolis: Cisco Press	• Standards
Chandra, P. (2002, May 23). 802.11 Security. Retrieved April 3, 2005, from http://www.wirelessdevnet.com/articles/80211security/	• WEP capability-authentication • WEP capability-encryption • WEP component-encryption • WEP vulnerability-encryption • WEP vulnerability-key management • WEP vulnerability-authentication
Cohen, A., & O'Hara, B. (2003, May 26). 802.11i shores up wireless security. [Electronic Edition]. Network World	• Standards • WPA Capability-key management • WPA component-key management • 802.11i component-encryption
Connolly, P. J. (2002, March 8). The trouble with 802.1x. Retrieved on March 23 from http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x	• Standards • EAP-TLS capabilities-authentication

Source	Topic Area
.html	• EAP-TLS vulnerability-authentication • EAP-TLS vulnerability-key management
DeBeasi, P. (2004, April). Wireless LAN Security Protocols. Wireless Design & Development, Vol. 12 Issue 4, p42, 3p, 2c	• Standards • WEP capability-authentication • WEP component-encryption • WEP vulnerability-encryption: • WEP vulnerability-authentication • WEP vulnerability-key management • WPA component-encryption • WPA component-key management • WPA vulnerability-authentication
Disabato, M. C. (2003, May). Wi-Fi Protected Access Finally Arrives. Business Communications Review, Vol. 33 Issue 5, p42, 5p	• WEP vulnerability-encryption
Dornan, A. (January 2004). EAP: Extending Authentication to the Wireless LAN. Network Magazine, Vol. 19 Issue 1, p38	• Standards • EAP-TLS component-authentication • EAP-TLS vulnerability-authentication • EAP-TLS capability-authentication • EAP-TLS component-encryption
Funk, P. (2005, March 28). The nuts and bolts of 802.11i wireless LAN security. WEP wasn't good enough, but 802.11i does the job. Retrieved April 2, 2005, from http://www.techworld.com/security/features/index.cfm?FeatureID=1293	• EAP-TLS component-authentication • 802.11i capability-encryption
Gain, B. (2001, August 8). As wireless LAN grows, so do security concerns. EBN, Issue 1277	• WEP vulnerability-encryption

Source	Topic Area
Garcia, A. (2005, January 3). 802.11i Strengthens Wi-Fi Security. EWeek Magazine	• 802.11i capability-encryption • 802.11i capability-authentication
Geier, J. (2003, May 7). 802.1X Offers Authentication and Key Management. Retrieved on March 23, 2005 from **http://www.wifiplanet.com/tutorials/article.php/1041171**	• WEP capability-encryption • WEP vulnerability-encryption • WEP vulnerability-key management • EAP-TLS capability-authentication • EAP-TLS capability-key management
Griffith, E. (2004, June 25). 802.11i Security Specification Finalized. Obtained on March 29 from http://www.wifiplanet.com/news/article.php/3373441	• WEP vulnerability-encryption • WPA capability-authentication • WPA component-key management • WPA component-authentication • 802.11i capability-encryption
Halasz, D. (2004, August 25). IEEE 802.11i and wireless security. Retrieved on March 23 from http://www.embedded.com//showArticle.jhtml?articleID=34400002	• Standards • WEP vulnerability-encryption • WEP vulnerability-encryption • EAP-TLS capability-authentication
Huckaby, T. (2001, December). Is 802.1x the Answer? [Electronic Version]. Windows IT Pro, December 2001	• Standards • EAP-TLS capability-encryption • EAP-TLS capability-authentication • EAP-TLS component-authentication
Javvin Company (n.d). IEEE 802.11i: WLAN Security Standards. Retrieved April 2, 2005 from http://www.javvin.com/protocol80211i.html	• Standards
Molta, D. (2002, February 4). WLAN Security On The Rise.	• WEP component-

Source	Topic Area
Network Computing, Vol. 13 Issue 3, p86, 4p	encryption • WEP vulnerability-key management • WEP vulnerability-encryption • WEP component-authentication • EAP-TLS capability-authentication • EAP-TLS component-authentication
Mooney, E. V.(2002, August 19). WLAN security oxymoron. RCR Wireless News, Vol. 21 Issue 33, p12, 1p, 4c	• WEP vulnerability-key management • WEP vulnerability-encryption • 802.11i component-encryption
Motsay, E. (2004, August 2). Standards move forward but security vulnerabilities, risks remain. RCR Wireless News, Vol. 23 Issue 31, p8, 1p	• 802.11i component-encryption
Nair, R. (2003, November). Minimize the risk of wireless exposure. Communications News, Vol. 40 Issue 11, p32, 2p	• WEP vulnerability-encryption
Omatseye, S. (2003, May 5). Wi-Fi Alliance locks up new security standard. RCR Wireless News, Vol. 22 Issue 18	• Standards • WPA component-encryption • WPA capability-encryption
Ou, G. (2002, September 3). At last, real wireless LAN security: Introducing 802.1x and EAP. TechRepublic	• WEP vulnerability-key management • EAP-TLS capability-authentication • EAP-TLS component-authentication • EAP-TLS capability-key management
Pabrai, A, & Uday, O. (2004, October). Securing Wireless Networks. Certification Magazine, Vol. 6 Issue 10, p34-36	• Standards • WEP component-authentication • WEP capability-encryption • EAP-TLS capability-authentication • WPA component-

Source	Topic Area
	encryption • WPA component-key management
Passmore, D. (2004, January). Treating WLAN Users as Hostile. Business Communications Review; Jan2004, Vol. 34 Issue 1, p14, 2p	• WEP vulnerability-encryption • WPA capability-key management • WPA capability-encryption
Roberts, P. (2003, November 7). Paper finds new wireless standard less secure. IDG News Service, 11/07/03	• WPA capability-authentication • WPA component-authentication • WPA vulnerability-authentication
Robinson, F. (2004, April 1). Examining 802.11i and WPA: The New Standards – Up Close. [Electronic Edition]. Network Computing Magazine	• Standards • WPA component-key management • WPA component-authentication
Roshan, P. (2001, September 24). 802.1X authenticates 802.11 wireless. Network World	• EAP-TLS capability-authentication • EAP-TLS component-authentication
searchMobileComputing.com Definitions (2003, May 9). 802.1X. Retrieved March 25, 2005, from http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci787174,00 html	• EAP-TLS capability-authentication • EAP-TLS component-authentication
Shinder, D. (2004, July 15). 802.11i, WPA, RSN and What it all Means to Wi-Fi Retrieved April 25, 2005, from http://www.windowsecurity.com/pages/article_p.asp?id=1345	• Standards • WPA component -key management • WPA component-authentication • WPA capability-authentication • WPA component-encryption • 802.11i component-encryption
Snyder, J. (2002, May 6). What is 802.1x? Network World Global Test Alliance Retrieved March 23, 2005, from	• EAP-TLS component-authentication • EAP-TLS capability-

Source	Topic Area
http://www.nwfusion.com/research/2002/0506whatisit.html	authentication
Snyder, J., & Thayer, R. (2004, October 4). 802.11i: The next big thing. Network World [Electronic Edition].	• 802.11i component-encryption
Snyder, J., & Thayer, R. (2004, October 4). 802.1X: A stepping stone. Network World. [Electronic Edition]	• EAP-TLS component-authentication • EAP-TLS capability-key management • EAP-TLS capability-encryption • EAP-TLS capability-authentication
Snyder, J. & Thayer, R. (2004, October 4). WPA - An accident waiting to happen. Network World [Electronic Version]	• Standards • WPA component-key management • WPA capability-key management • WPA component-encryption • WPA capability-authentication • WPA component-authentication • WPA vulnerability-authentication
Steinke, S. (2002, June). Lesson 167: Security and 802.11 Wireless Networks. Network Magazine; Jun2002, Vol. 17 Issue 6, p30, 2p, 1c	• WEP vulnerability-encryption • WEP component-encryption • WEP capability-encryption • WEP vulnerability- key management
Welcher, P. J. (2004, May). Examining 802.1x and EAP. Retrieved on March 23 from http://www.enterprisenetworksandservers.com/monthly/art.php/696	• Standards • EAP-TLS capability-authentication • EAP-TLS component-authentication
Wi-Fi Protected Access. Wikipedia. Retrieved on April 12, 2005 from http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access	• WPA component-key management • WPA capability-key management • WPA component-encryption

Source	Topic Area
	• WPA capability-authentication
Wildstrom, S. H. (2002, November 13). Stronger Security Fences for Wi-Fi. Business Week Online	• Standards • WEP vulnerability-encryption • WPA capability-authentication

Bibliography

Air Defense (2005). Wireless LANs: Six Steps for Enterprise & Regulatory Policy Compliance. Retrieved April 21, 2005, from www.airdefense.net

Albright, B. (2003, March). Wireless insecurity. Frontline Solutions, Vol. 4 Issue 3, p16-19

Andress, M. (2002, January 7). 802.11 wireless LANs. InfoWorld, Vol. 24 Issue 1, p36, 1/3p

Anonymous (2003, November). Minimize the risk of wireless exposure. Communications News, Vol. 40 Issue 11, p32, 2p

Arbaugh, W. A., & Edney, J. (2004). *Real 802.11 Security.* Boston: Pearson Education Inc.

Balinsky, A., & Miller, D., & Sankar, K., & Sundaralingam, S, (2005). Cisco Wireless LAN Security. Indianapolis: Cisco Press

Barrett, J. (2000, May 29). Consumer Privacy Looms As A Key Issue. National Underwriter / Property & Casualty Risk & Benefits, Vol. 104 Issue 22, p9, 2p

Bauer, M. (2005, April). Securing WLANs with WPA and FreeRADIUS, Part I. Linux Journal, Issue 132, p36, 3p, 2 diagrams

Berinato, S., & Scalet, S. (2002, March 20). The ABCs of Security. [Electronic Version]. CIO Magazine

Brewin, B. (2004, May 24). IT Managers Ready Defenses Against Flaw in Wireless LANs. Computerworld, Vol. 38 Issue 21, p14-17

Brewin, B. (2003, May 12). WLAN Security Still Vexes IT. Computerworld, Vol. 37 Issue 19, p1-2

Case, M. (2004, March 30). Is your network the weakest link? Computer Weekly, p27, 1/3p, 1c

Champness, A. (1998, March). Understanding the benefits of IEEE 802.11. Canadian Electronics, Vol. 13 Issue 2, p22, 1/2p, 1c

Chandra, P. (2002, May 23). 802.11 Security. Retrieved April 3, 2005, from http://www.wirelessdevnet.com/articles/80211security/

Cheek, P. (2005, March 24). Managing the Risks. New Media Age, Supplement, p3, 2/3p, 1c

Cheung, D. (2004, June). WLAN Security & Wi-Fi Protected Access. Dr. Dobb's Journal: Software Tools for the Professional Programmer, Vol. 29 Issue 6

CIO Insight (2004, December). Compliance Becomes a Top IT Priority. Special Issue Issue 48, p58, 1p

Cohen, A., & O'Hara, B. (2003, May 26). 802.11i shores up wireless security. [Electronic Edition]. Network World

Connolly, P. J. (2002, March 8). The trouble with 802.1x. Retrieved on March 23 from http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x.html

Davies, P. (2003, December). Companies clamping down on wireless workers who bypass encryption. Workforce Management, Vol. 82 Issue 13, p69, 3p, 1c

DeBeasi, P. (2004, April). Wireless LAN Security Protocols. Wireless Design & Development, Vol. 12 Issue 4, p42, 3p, 2c

Disabato, M. C. (2003, May). Wi-Fi Protected Access Finally Arrives. Business Communications Review, Vol. 33 Issue 5, p42, 5p

Dix, J. (2004, October 11). Doing the compliance two-step. Network World, Vol. 21 Issue 41, p36, 1/3p

Dodds, R., & Hague, I. (2004, December). Information security--more than an IT issue? Chartered Accountants Journal, Vol. 83 Issue 11, p56, 2p

Dornan, Andy (January 2004). EAP: Extending Authentication to the Wireless LAN. Network Magazine, Vol. 19 Issue 1, p38

Economist (2004, June 12). A brief history of Wi-Fi. Vol. 371, Issue 8379, special section p26, 2p, 1 graph, 1c

Economist, The (2002, October 26). When the door is always open. Vol. 365 Issue 8296, p16, 2p, 1 graph, 1c

Ferguson, R. B. (2005, March 31). Making Sense of Sarbanes-Oxley Compliance Requirements Retrieved March 31, 2005 from http://www.eweek.com/article2/0,1759,1780927,00.asp?kc=EWRSS03119TX1 0000594

Funk, P. (2005, March 28). The nuts and bolts of 802.11i wireless LAN security. WEP wasn't good enough, but 802.11i does the job. Retrieved April 2, 2005, from http://www.techworld.com/security/features/index.cfm?FeatureID=1293

Gain, B. (2001, August 8). As wireless LAN grows, so do security concerns. EBN, Issue 1277

Garcia, A. (2005, January 3). 802.11i Strengthens Wi-Fi Security. EWeek Magazine

Garcia, A. (2003, Fall). Enterprise Managed WLAN Products. PC Magazine, Vol. 22 Issue 18, p82, 2p, 1 chart

Garretson, C. (2003, September 1). Under the gun. Network World, Vol. 20 Issue 35, p38, 2p

Gast, M. (2002). 802.11 Wireless Networks: The Definitive Guide. Sebastopol: O'Reilly & Associates

Geier, J. (2003, May 7). 802.1X Offers Authentication and Key Management. Retrieved on March 23, 2005 from http://www.wifiplanet.com/tutorials/article.php/1041171

Goodwin, B. (2004, April 27). Wi-Fi dangers must be tackled by the board. Computer Weekly, p5, 1/8p

Greene, T. (2003, June 23). Cautious users cast wary eye on WLANS. Network World, Vol. 20 Issue 25, p17-18

Griffith, E. (2004, June 25). 802.11i Security Specification Finalized. Obtained on March 29 from http://www.wi-fiplanet.com/news/article.php/3373441

Halasz, D. (2004, August 25). IEEE 802.11i and wireless security. Retrieved on March 23 from http://www.embedded.com//showArticle.jhtml?articleID=34400002

Heffes, E. M. (2005, March). Privacy Issues: Getting Noticed. Financial Executive, Vol. 21 Issue 2, p30-32

Hollis, E. (Dec 2004). WLAN Switching: Managing Wireless Access Points. Certification Magazine, Vol. 6 Issue 12, p 42

Huckaby, T. (2001, December). Is 802.1x the Answer? [Electronic Version]. Windows IT Pro, December 2001

IETF, (1999, October). RFC 2716 - PPP EAP TLS Authentication Protocol. Internet RFC/STD/FYI/BCP Archives. Retrieved April 12, 2005, from http://www.faqs.org/rfcs/rfc2716.html

IETF, (1999, October). RFC 2246 - The TLS Protocol Version 1.0. Internet RFC/STD/FYI/BCP Archives. Retrieved April 13, 2005, from http://www.faqs.org/rfcs/rfc2246.html

Jason T. (2003, February 5). Security for wireless networking. New Straits Times Malaysia)

Javvin Company (n.d). IEEE 802.11i: WLAN Security Standards. Retrieved April 2, 2005 from http://www.javvin.com/protocol80211i.html

Johnson, M. (2004, March 22). Privacy Hostages. Computerworld, Vol. 38 Issue 12, p22, 2/3p

Kim, D. S., & Kittipom, P. & Porter, J. D. (2005, March). Performance evaluation of heterogeneous wireless local area networks. Computers & Industrial Engineering, Vol. 48 Issue 2, p251, 21p

Klassen, K. (2004, November). Wireless security is evolving. Communications News, Vol. 41 Issue 11, p6

Krippendorff, K. (2004). *Content Analysis.* Thousand Oaks: Sage Publications Inc.

Kumar, J. (2005, April 11). Strategic Security. Computerworld, Vol. 39 Issue 15, p48, 1p

Le Thomas, N. (2004, July 15). Can wi-fi live up to enterprise? America's Network, Vol. 108 Issue 11, p30, 2p, 2c

Leedy, P. D., & Ormrod, J. E. (2001). *Practical Research Planning and Design.* Upper Saddle River: Prentiss-Hall Inc.

Marek, S. (2001, October 22). Wireless' Weakest Link. Wireless Week, Vol. 7 Issue 43, p26, 1p

Mastroberte, T. (2003, June 16). Risky Business.Convenience Store News, Vol. 39 Issue 7, p107, 4p, 4c

Messmer, E. (2003, February 14). White House issues 'National Strategy to Secure Cyberspace'. Retrieved April 23, 2005, from http://www.nwfusion.com/news/2003/0214ntlstrategy.html

Molta, D. (2005, February 17). WLANs Bust Out. Network Computing, Vol. 16 Issue 3, p37-42

Molta, D. (2002, February 4). WLAN Security On The Rise. Network Computing, Vol. 13 Issue 3, p86, 4p

Mooney, E. V.(2002, August 19). WLAN security oxymoron. RCR Wireless News, Vol. 21 Issue 33, p12, 1p, 4c

Motsay, E. (2004, August 2). Standards move forward but security vulnerabilities, risks remain. RCR Wireless News, Vol. 23 Issue 31, p8, 1p

Nair, R. (2003, November). Minimize the risk of wireless exposure. Communications News, Vol. 40 Issue 11, p32, 2p

Nelson, B. (2004, June). Wireless security choices. Communications News, Vol. 41 Issue 6, p32

Omatseye, S. (2003, May 5). Wi-Fi Alliance locks up new security standard. RCR Wireless News, Vol. 22 Issue 18

Ou, G. (2002, September 3). At last, real wireless LAN security: Introducing 802.1x and EAP. TechRepublic

Pabrai, A, & Uday, O. (2004, October). Securing Wireless Networks. Certification Magazine, Vol. 6 Issue 10, p34-36

Pabrai, A., & Uday, O. (2003, May). Wireless Security. Certification Magazine, Vol. 5 Issue 5, p26-27

Palmquist, Mike, et al. (2005). Content Analysis. Writing@CSU. Colorado State University Department of English. Retrieved [Date] from http://writing.colostate.edu/references/research/content/.

Parenty, T. J. (2003). *Digital Defense: What You Should Know About Protecting Your Company's Assets.* Boston: Harvard Business School Press

Passmore, D. (2004, January). Treating WLAN Users as Hostile. Business Communications Review; Jan2004, Vol. 34 Issue 1, p14, 2p

RCR Wireless News (2004, February 2). WLAN growth expected to continue through 2006. Vol. 23 Issue 5, p21, 1/9p

Reed, C. (2004, February 10). Securing a wireless network means much more than just protecting against hackers. Computer Weekly, p30

Riezenman, M. J. (2002, September). The ABCs of IEEE 802.11. IEEE Spectrum, Vol. 39 Issue 9, p20, 1/2p

Rist, O. (2005, March 21). Attack of the Auditors. InfoWorld, Vol. 27 Issue 12, p36, 6p, 1 diagram, 1c

Roberts, P. (2003, November 7). Paper finds new wireless standard less secure. IDG News Service, 11/07/03

Robinson, F. (2004, April 1). Examining 802.11i and WPA: The New Standards – Up Close. [Electronic Edition]. Network Computing Magazine

Roshan, P. (2001, September 24). 802.1X authenticates 802.11 wireless. Network World

Schwartz, E. (2004, December 13). Getting Serious With Wi-Fi. InfoWorld, Vol. 26 Issue 50, p12, 1p

searchMobileComputing.com Definitions (2003, May 9). 802.1X. Retrieved March 25, 2005, from http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci787174,00 html

Shinder, D. (2004, July 15). 802.11i, WPA, RSN and What it all Means to Wi-Fi Retrieved April 25, 2005, from http://www.windowsecurity.com/pages/article_p.asp?id=1345

Snyder, J. (2002, May 6). What is 802.1x? Network World Global Test Alliance Retrieved March 23, 2005, from http://www.nwfusion.com/research/2002/0506whatisit.html

Snyder, J., & Thayer, R. (2004, October 4). 802.11i: The next big thing. Network World [Electronic Edition].

Snyder, J., & Thayer, R. (2004, October 4). 802.1X: A stepping stone. Network World. [Electronic Edition]

Snyder, J., & Thayer, R. (2004, October 4). Cracking the wireless security code. Network World [Electronic Version]

Snyder, J. & Thayer, R. (2004, October 4). WPA - An accident waiting to happen. Network World [Electronic Version]

Steinke, S. (2002, June). Lesson 167: Security and 802.11 Wireless Networks. Network Magazine; Jun2002, Vol. 17 Issue 6, p30, 2p, 1c

Tolly, K. (2005, March 28). Identity theft, data security, back-up services. Network World, Vol. 22 Issue 12, p18, 1/3p

Vijayan, J. (2004, June 14). Gartner Sees Growing Need For Wireless Security Policies. Computerworld, Vol. 38 Issue 24, p8, 1/3p

Vijayan, J. (2003, October 6). Laws, Concern for Corporate Image Make Privacy A Priority. Computerworld; 10/6/2003, Vol. 37 Issue 40, p12, 3/4p

Vijayan, J. (2003, May 26). IT Risks, Physical Threats Change Corporate Approaches to Security. Computerworld, Vol. 37 Issue 21, p12, 1/3p

Webb, R. (2003, July). Wireless LAN reality check. Telecommunications – International Edition, Vol. 37 Issue 7, p23, 3p

Welcher, P. J. (2004, May). Examining 802.1x and EAP. Retrieved on March 23 from http://www.enterprisenetworksandservers.com/monthly/art.php/696

Wi-Fi Protected Access. Wikipedia. Retrieved on April 12, 2005 from http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Wildstrom, S. H. (2002, November 13). Stronger Security Fences for Wi-Fi. Business Week Online